DOI 10.37882/2223-2974.2026.02.01

ПОВЫШЕНИЕ РИСКОВ СОВЕРШЕНИЯ ДОЛЖНОСТНЫХ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ НОВЫХ ЦИФРОВЫХ ПРАКТИК ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

INCREASING RISKS OF COMMITTING OFFICIAL CRIMES IN THE CONTEXT OF NEW DIGITAL PRACTICES OF PUBLIC ADMINISTRATION

T. Bauer

Summary. The article is devoted to the analysis of the impact of digital public administration practices, formed in the process of transferring a number of state functions into information systems, on the possibility of committing official crimes and crimes in the field of computer information. Key trends and approaches to the automation of the activities of public authorities and other organizations involved in the provision of unified digital services are examined, which contribute to an increase in the criminogenic nature of the information sphere. The methodological basis includes an analysis of established state and business approaches to the organization of end-to-end digital services, current legislation regulating the field of information technologies, and judicial practice concerning crimes in the digital environment. The obtained results may be useful for specialists in the field of public administration and information security.

Keywords: public administration, information technologies, information security, information systems, digital services, crimes in the sphere of public administration, official crimes, crimes in the sphere of computer information.

Бауэр Татьяна Андреевна
Старший преподаватель,
Национальный исследовательский университет «Высшая школа экономики»
bauer@spb.hse.ru

Аннотация. Статья посвящена анализу влияния цифровых практик государственного управления, сложившихся в процессе перевода ряда государственных функций в информационные системы, на возможность совершения должностных преступлений и преступлений в сфере компьютерной информации. Рассмотрены ключевые тенденции и подходы к автоматизации деятельности органов власти и иных организаций, задействованных в оказании единых цифровых услуг, способствующие повышению криминогенности информационной сферы. Методологическая основа включает анализ сложившихся государственных и бизнес-подходов к организации «сквозных» цифровых сервисов, действующего законодательства, регулирующего сферу информационных технологий, судебной практики по преступлениям в цифровой среде. Полученные результаты могут быть полезны для специалистов в области государственного управления и информационной безопасности.

Ключевые слова: государственное управление, информационные технологии, информационная безопасность, информационные системы, цифровые сервисы, преступления в сфере государственного управления, должностные преступления, преступления в сфере компьютерной информации.

Начиная с середины 2000-х годов Российская Федерация стремительно движется по пути информатизации. Информационные технологии продвигаются как на базе государства, так и в бизнесе.

Информатизация (производственные процессы в данной статье рассмотрены не будут) включает в себя не только автоматизацию рутинных процессов с участием человека, но и сбор, обработку, использование большого объема данных о пользователях информационных систем в целях создания оптимальных процессов продвижения товаров и услуг, включая государственные услуги, формирования информационных платформ, объединяющих миллионы участников.

Основной тенденцией последних лет также стала концентрация данных о пользователях из разных информационных систем в «одних руках» — либо органа власти (например, Минцифры России и ПАО Ростелеком — развивают проект «Госуслуги», Банка России и крупных кредитных учреждений — проект «Цифровой профиль гражданина»), либо владельца ИТ-платформ (например, цифровая платформа Ozon, банковские информационные системы ПАО Сбербанк, Банка ВТБ (ПАО)).

При этом при создании таких «сквозных» информационных систем и цифровых сервисов как органы власти, так и бизнес, ориентируются на собственные разнородные проекты и показатели результативности. Создание единообразных правил разработки, использования и защиты информационных систем — как объекта технической инфраструктуры, и их содержания — пользовательских данных, в связи с вышеизложенными подходами затруднено.

В настоящее время сферу информационных технологий регулирует широкий перечень нормативных правовых актов из различных сфер правоотношений (более 7 только федеральных законов), включая многочисленные нормы, вводящие экспериментальные режимы для

апробации информационных технологий и искусственного интеллекта. Наиболее важными из них являются федеральные законы от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3], от 27.07.2006 № 152-ФЗ «О персональных данных» [4], от 26.07.2017 № 187-ФЗ.

«О безопасности критической информационной инфраструктуры Российской Федерации» [2], приказы ФСБ и ФСТЭК по защите информационных систем и информации.

При этом вновь вводимые законодательные нормы по-прежнему базируются на понятиях, определения и принципах, которые были выработаны до появления большей части современных технологий, перестроивших процессы взаимодействия государства, бизнеса, граждан.

Основным ограничением на пути определения актуальных правовых рамок цифровизации и связанного с ней разграничения функций, полномочий, прав и обязанностей ее участников: органов власти, организаций и граждан, является сложность, многоуровневость, многосоставность «цепочек» информационных систем, задействованных в предоставлении каждой цифровой услуги, а также постоянная изменчивость функциональной, технической и технологической конфигурации как каждой информационной системы в отдельности, так и их совокупности. В свою очередь такая внутренняя конфигурация цифровых услуг порождает сложные правовые модели взаимодействия операторов различных информационных систем, их сотрудников, организаций, оказывающих услуги таким операторам (от разработки программного обеспечения до предоставления услуг удаленного колл-центра), органов, предоставляющих государственные услуги с использованием своих или сторонних информационных систем, пользователей и органов власти, реализующих правоохранительные и контрольно-надзорные функции.

При этом правовые сложности и неопределенность возникают не только с распределением прав, обязанностей, ответственности между участниками «цепочки» информационных систем, но с корректным использованием, маршрутизацией, анализом потоков данных, которые поступают в такие информационные системы. Накопление массивов данных во взаимосвязанных информационных системам, влечет появление у их операторов — органов власти или организаций, а также у их обслуживающих организаций, возможности технического доступа ко всему массиву данных, циркулирующему внутри информационной «цепочки». Как правило такой обмен информацией не поддаётся исчерпывающему юридическому закреплению и контролю, что неизбежно приводит всех его участников, включая должностных лиц и сотрудников органов власти к выходу за пределы своих прав и полномочий, использованию не принадлежащих им данных, в том числе для смежных или вообще ранее нигде юридически не предусмотренных действий.

Рассмотрим вышеприведенную проблематику в части деятельности органов власти и их представителей при использовании информации и информационных систем, с точки зрения действующего уголовного законодательства.

Так глава 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса Российской Федерации (далее — УК РФ) [1] содержит описание ряда составов преступлений, которые охватывают в том числе действия должностных лиц и сотрудников органов власти, связанных с неправомерным доступом к информации и эксплуатацией систем:

— объективной стороной преступления, предусмотренного статья 272 УК РФ [1], является неправомерный доступ к компьютерной информации, сопряженный с ее уничтожением, блокированием, модификацией либо копированием. По мнению автора, при определении правомерности доступа должностного лица или сотрудника органа власти в информационную систему следует понимать совокупность нормативных правовых актов, во-первых, предоставляющих органу власти право использования такой информационной системы сообразно с его функциями и полномочиями, во-вторых, определяющих какие именно полномочия и задачи органа власти решаются за счет использования функционала или информации конкретной информационной системы, в-третьих, определяющих цели, задачи, функционал, перечень информации, находящейся в информационной системе, правомочных пользователей и условия использования ими информации, содержащейся в информационной системе, и наконец, в-четвертых, вытекающих из всех выше обозначенных нормативных актов, правил доступа к такой информации путем использования набора технологий и технических средств, должностных инструкций. Принимая во внимание, что указанное преступление является оконченным с момента совершения перечисленных в статье действий с информацией, но руководствуясь рекомендациями постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» [5] о необходимости установления иных действий с информацией,

к которой был получен неправомерный доступ, целесообразно выяснять какая именно информация была извлечена из информационной системы, была ли указанная информация использована должностным лицом или сотрудником в личных корыстных целях или же для выполнения иных служебных обязанностей, которые однако де-юре никак не связаны с возможностью использования конкретных данных. Такой подход, по мнению автора, во-первых, позволит дать деянию верную квалификацию, в том числе одновременно квалифицировать действия субъекта преступления также по статьям 285, 285.3, 286, 159 УК РФ [1], во-вторых, позволит выявлять недостатки правового регулирования как в нормативных правовых актах, регламентирующих полномочия органов власти, так и актов, позволяющих использование тех или иных массивов защищаемых данных в целях исполнения сотрудниками органов власти своих должностных обязанностей;

— объективная сторона преступления, предусмотренного статьей 272.1 УК РФ [1], заключается в незаконной обработке персональных данных, полученных путем неправомерного доступа к средствам ее обработки либо иным незаконным путем. Таким образом, по мнению автора, исходя из ранее указанной проблематики сложно контролируемого перетока данных из одной взаимосвязанной системы в другую может потребоваться установить не только незаконность доступа должностного лица в информационную систему, содержащую персональные данные, например, когда у него отсутствуют такие полномочия, но и то, что персональные данные находятся в данной информационной системе правомерно. Однако стоит обратить внимание, что в случае с пользователями информационных систем, получившими доступ в систему правомерно, но воспользовавшимися данными, которые не должны были находиться в такой информационной системе, ответственность за наполнение информационной системы должно нести другое лицо — оператор системы или орган власти, ответственный за ее информационное наполнение;

— статьей 274 УК РФ [1] предусмотрено наказание за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Не останавливаясь на правилах эксплуатации, так как они лежат в большей части в технической сфере и сфере информационной безопасности, отмечу, что правила доступа являются естественным продолжением правовой конструкции по наделению органа власти в целом и должностного лица или сотрудника в частности полномочиями по использованию информации, содержащейся в информационной системе. С другой стороны, правила доступа для внутренних самообслуживаемых систем органа власти (например, система внутреннего электронного документооборота) могут иметь более простую правовую структуру и представлять собой только должностные инструкции и ролевые модели доступа для сотрудников и администраторов системы;

— в целях корректной квалификации действий субъекта преступления, предусмотренного частями 2 и 3 статьи 274.1 УК РФ [1], кроме вышеописанных прав доступа к информации в информационной системе или самой информационной системе, в том числе если она представляет собой автоматизированную систему управления какими-либо процессами органа власти, по мнению автора, необходимо четко определить границы информационной системы, как объекта критической информационной инфраструктуры (КИИ), изучить акт категорирования на такую информационную систему и убедиться, что ее части, через которые был осуществлен несанкционированный доступ находились в периметре защищаемого контура и соответственно в зоне ответственности оператора системы и конкретных должностных лиц.

Действия, совершенные субъектом преступлений, предусмотренных статьями 274 и 274.1 УК РФ [1], также могут быть квалифицированы по статьям УК РФ, предусматривающим должностные и корыстные преступления в зависимости от мотива и последствий их совершения, что составит идеальную совокупность преступлений.

Анализ судебной практики [7-14] показал, что в настоящее время наиболее распространенными преступления должностных лиц и сотрудников органов власти в области неправомерного доступа и использования информации из информационных систем является корыстная заинтересованность в передаче данных третьим лицам за вознаграждение, как правило, это специализированные информационные системы конкретных ведомств. При этом должностное лицо или сотрудник или имел санкционированный допуск в систему, однако использовало информацию из нее за пределами своих должностных обязанностей, либо использовал незаконно своих коллег или их средства доступа в информационные системы. Однако приговоры судов в большинстве случае не содержат описания и оценки содержания и значимости самой информации, в отношении которой совершались неправомерные действия, хотя оцен-

ка причиненного или потенциального ущерба входит в квалифицирующие признаки ряда вышеприведенных преступлений.

При этом необходимо учитывать, что такой несанкционированный доступ, особенно с использованием специализированного вредоносного программного обеспечения, к «цепочке» информационных систем, может приводить к получению не только информации, используемой в деятельности конкретного ведомства, но и дать возможность получения данных из других государственных информационных систем. Одновременно, несанкционированный доступ к информации из смежных информационных систем, при условии недостаточного учета и прозрачности передачи данных по «цепочке», может привести к отсутствию фиксации факта их утери, искажения или копирования и, как следствие, к невозможности их восстановления или верификации, а также привлечения виновных лиц к ответственности.

На основании вышеизложенного, с учетом глобального влияния цифровизации на сектор государственного управления, интеграции государственных, ведомственных и коммерческих систем в целях оказания единых услуг гражданам и организациям, а также стремлению органов власти перейти на модель принятия решений на основе данных, становится очевидным, что сохранение законности использования информации, ее целостности и достоверности является не только задачей уголовного законодательства, как крайней меры воздействия на участников информационных правоотношений, но и мер превентивных, профилактических, лежащих в данном случае в плоскости установления единых принципов, норм и правил создания и использования органами власти информационных систем, четкого и однозначного распределение полномочий и прав на использование информации.

Так изучая сложившуюся практику использования государственных информационных систем, в том числе результаты проверки Счетной Палатой Российской Федерации эффективности использования бюджетных средств на создание государственных и ведомственных информационных систем от 2022 года [6], очевидно, что создаваемые системы не только оцифровывают государственные функции ранее существовавшие, но и создают возможности реализации на базе собираемых данных новых, ранее не относящиеся к данному органу власти полномочия. Кроме того, указанные в документах цели и функции систем зачастую не отражают тех возможностей, которыми обладает информационная система, таким образом, создаются дополнительные стимулирующие факторы, способствующие совершению преступлений в сфере информационных технологий в органах власти. К таким факторам также можно отнести: максимально легкий доступ должностных лиц и сотрудников органов власти к большому объему данных, в том числе не обоснованный полномочиями такого органа власти и (или) сотрудника (при иных условиях сотрудник такой органа ни при каких обстоятельствах не имел бы доступ к такому большому набору данных); низкий уровень вовлеченности рядовых сотрудников в процессы обеспечения информационной безопасности; низкие заработные платы и квалификация рядовых сотрудников, допущенных до работы в информационных системах; отсутствие психологической ответственности сотрудников за незаконное использование защищаемых данных, ввиду легкости их доступности и неосязаемости границ своих служебных полномочий в этой части; совмещение в одном юридическом лице или органе власти многих функций, позволяющих собирать большие и разнообразные сведения о физических и юридических лицам, иных органах власти, их деятельности.

В целях упорядочивания информатизации государственного сектора целесообразно использовать следующие подходы правового регулирования:

1. Ввести в законодательство об информации и информационных системах самостоятельные понятия «государственная информационная система», конкретизирующее цели создания государственных информационных систем, а также «государственная цифровая платформа», «государственный информационный ресурс» и «ведомственная информационная система».
2. Определить закрытый перечень видов нормативных правовых актов, являющихся основанием для создания государственных и ведомственных информационных систем.
3. Однозначно закрепить виды государственных и ведомственных информационных систем (федеральные государственные информационные системы и региональные государственные информационные системы).
4. Перечень целей, типовых задач и функций органов власти, органов местного самоуправления и подведомственных им организаций подлежащих реализации в таких информационных системах установить нормативными правовыми актами уровня, соответствующего уровню информационной системы.
5. Законодательно зафиксировать четкое требование о соотнесении целей и задач информационных систем и содержащейся в них информации с целями и задачами органов власти, регламентировать подход к оценке необходимость использования единых баз данных («озер данных») различными органами власти и организациями, с учетом вышеописанных рисков и наличия потенциальных возможностей неправомерного доступа сотрудников к охраняемой законом информации, принадлежащей разным субъектам данных.

Подводя итог, можно отметить, что цифровизация не только расширяет управленческие горизонты для органов власти, но и требует от них доскональной ранее невиданной проработки процессов принятия решений, основанных на данных, разработки четких однозначных алгоритмов верификации и сохранения данных, регламентированного соотнесение собираемых данных своим целям и задачам, организации мер информационной безопасности, обучения сотрудников.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. N63-ФЗ (с изм. и доп., вступ. в силу с 01.09.2025). Доступ из справ.-правовой системы «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_10699/.
2. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 г. N187-ФЗ (с изм. и доп.). Доступ из справ.-правовой системы «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_220885/.
3. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. N149-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_61798/.
4. О персональных данных: федер. закон от 27 июля 2006 г. N152-ФЗ (с изм. и доп.). Доступ из справ.-правовой системы «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_10699/.
5. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N37. Доступ из справ.-правовой системы «КонсультантПлюс»: https://www.consultant.ru/document/cons_doc_LAW_434573/#dst100004.
6. Бюллетень Счетной палаты РФ № 8(297)2022. https://www.sptulobl.ru/law/Bul-8-2022.pdf (дата обращения: 28.08.2025).
7. Приговор Преображенский районный суда города Москвы от 14 апреля 2022 года по делу № 1-363/22. https://mos-gorsud.ru/rs/preobrazhenskij/cases/docs/content/abdde270-bc00-11ec-a4b7-97f8b83ff5d4 (дата обращения: 28.08.2025).
8. Приговор Сафоновского районного суда Смоленской области от 27 февраля 2025 года по делу № 1-50/2025, УИД67RS0007-01-2024-003644-53. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOCN&n=14896394&cacheid=61EBE6214F87C1A541A5FE82115447C5&mode=splus&rnd=Pg2zcw#UyTzcvUTaK825pSI (дата обращения 27.08.2025).
9. Приговор Слободского районного суда Кировской области от 13 февраля 2025 года по делу № 1-37/2025, УИД: 43RS0034-01-2025-000100-73. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOPV&n=13641811&cacheid=9DE45989815714F1295B28CD62AD1304&mode=splus&rnd=Pg2zcw#uSM1dvUgnB4aLdAP1 (дата обращения 27.08.2025).
10. Приговор Саровского городского суда Нижегородской области от 16 октября 2019 года по делу N 1–166/2019. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOKI&n=7231933&cacheid=48F7D6D05D6854635F3B8334565DAD8F&mode=splus&rnd=Pg2zcw#K5tscvU9i6vgRSCd (дата обращения 25.08.2025).
11. Приговор Кировского районного суда города Самары от 28 февраля 2023 года по делу N 1–11/2023. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOPV&n=12562216&cacheid=6F44308FF87D16BAFED5A9992EB71612&mode=splus&rnd=Pg2zcw#sP9xcvUUBnNOfOIm1 (дата обращения 25.08.2025).
12. Приговор Кстовского городского суда Нижегородской области от 22 февраля 2024 N 1–25/2024. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOKI&n=12045344&cacheid=D53947350F6E4C42CFD40E2E5AAD65B5&mode=splus&rnd=Pg2zcw#9y0ycvU2hbXbfzMm (дата обращения 25.08.2025).
13. Приговор Лыткаринского городского суда Московской области от 11 апреля 2023 N 1–18/2023. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOKI&n=11476589&cacheid=E1272C4C5EDB358B1F4F2B69717AD35D&mode=splus&rnd=Pg2zcw#ttTycvUcHNYkOSZA2 (дата обращения 25.08.2025).
14. Приговор Мытищинского городского суда Московской области от 4 июня 2025 года N 1–275/2025. Доступ из справ.-правовой системы «КонсультантПлюс» по подписке: https://docs7.online-sps.ru/cgi/online.cgi?req=doc&base=AOKI&n=13287622&cacheid=21EFCC7B52B0B918DFD7D4C7D6134A0F&mode=splus&rnd=Pg2zcw#csuycvUK8kLar4x22 (дата обращения 25.08.2025).

Журнал «Современная наука: актуальные проблемы теории и практики»